

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-125022

(43)Date of publication of application : 25.04.2003

(51)Int.Cl. H04L 29/08
H04L 12/56

(21)Application number : 2001-320112

(71)Applicant : SONY CORP

(22)Date of filing : 18.10.2001

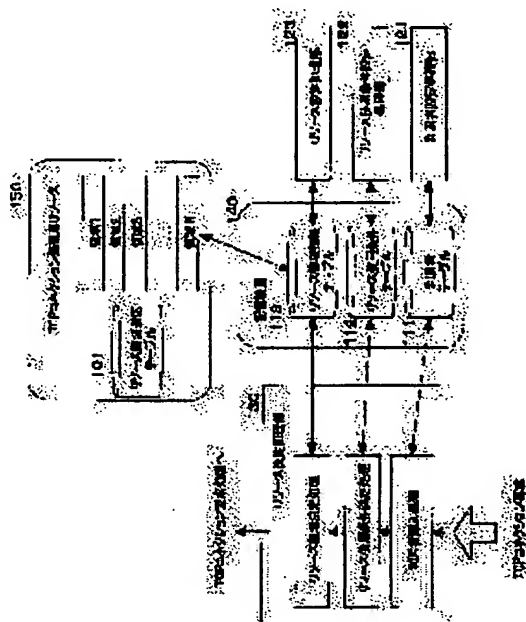
(72)Inventor : NAGANO MOTOHIKO

(54) COMMUNICATION PROCESSOR, COMMUNICATION PROCESSING METHOD AND COMPUTER PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication processor enabling such a connection control as limitation of resources in executed depending on the user.

SOLUTION: A user requesting connection is identified and a resource region being used according to use conditions of resources, which are set depending on the identified user, is determined. In a communication processor receiving connection requests from many and unspecified users through such a processing as setting much resources available for a high priority user, connection can be established preferentially for a specified user. The user is discriminated based on a received SYN packet and then connection is established based on the resource region or the number of connections which is set in correspondence with the discriminated user.



LEGAL STATUS

[Date of request for examination] 21.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3663627

[Date of registration] 08.04.2005

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-125022

(P2003-125022A)

(43) 公開日 平成15年4月25日 (2003.4.25)

(51) Int.Cl.⁷

H 0 4 L 29/08
12/56

識別記号

F I

H 0 4 L 12/56
13/00

テーマコード(参考)

A 5 K 0 3 0
3 0 7 A 5 K 0 3 4

審査請求 未請求 請求項の数19 O L (全 22 頁)

(21) 出願番号 特願2001-320112(P2001-320112)

(22) 出願日 平成13年10月18日 (2001. 10. 18)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 長野 元彦

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

Fターム(参考) 5K030 GA03 GA11 HA08 JT03 KA04

KA13 LB01 LB17 LB19

5K034 AA05 AA19 FF02 HH17 HH48

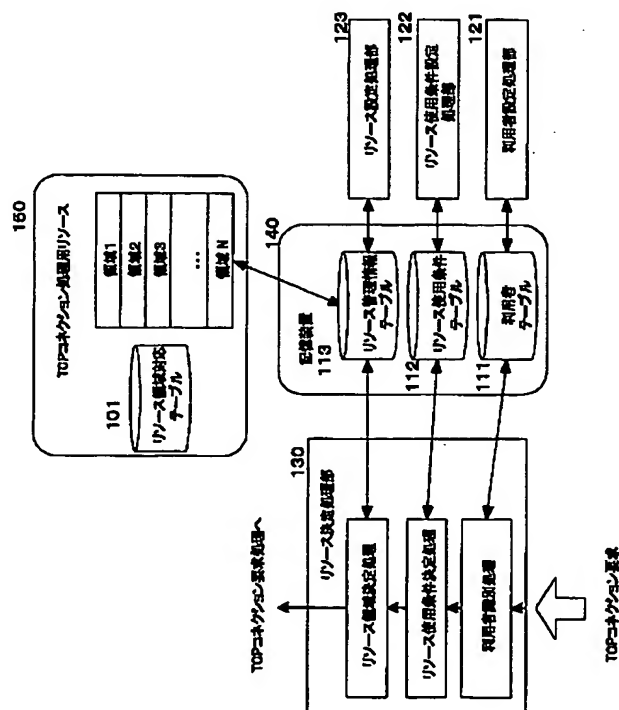
LL01

(54) 【発明の名称】 通信処理装置、および通信処理方法、並びにコンピュータ・プログラム

(57) 【要約】

【課題】 利用者に応じたリソース制限を実行したコネクション制御を可能とした通信処理装置を提供する。

【解決手段】 コネクション要求の利用者を識別し、識別された利用者に応じて設定されたリソースの使用条件に従って使用するリソース領域を決定する。優先度の高い利用者を使用可能なリソースを多く設定する処理により、不特定多数の利用者からのコネクション要求がある通信処理装置において、特定のユーザに対して優先的にコネクションを確立することが可能となる。受信 SYN パケットに基づいて利用者を判別し、判別した利用者に対応して設定されたリソース領域あるいはコネクション数に基づいてコネクションの確立を行なう。



1

【特許請求の範囲】

【請求項 1】通信コネクション要求を受信し、コネクション確立処理を実行する通信処理装置において、コネクション要求に対するコネクション確立可否の決定処理を実行する制御手段を有し、

前記制御手段は、

コネクション要求データに基づいて、コネクション要求元に対応する利用者の識別処理を実行し、該利用者識別処理において識別された利用者識別子に対応して設定された通信処理用リソースの空きを確認を条件としてコネクション確立処理を実行する構成を有することを特徴とする通信処理装置。

【請求項 2】前記通信処理用リソースは、複数の領域に分割されたメモリまたは記憶装置の記憶領域を含み、

前記通信処理装置は、

コネクション要求元に対応する利用者識別子と、前記記憶領域の各々とを対応付け、利用者毎の使用可能な記憶領域を設定したリソース使用条件テーブルを有し、

前記制御手段は、

前記利用者識別処理に基づいて識別された利用者に基づいて、リソース使用条件テーブルの検索を実行して、利用可能なリソースとしての記憶領域の判別を実行する構成であることを特徴とする請求項 1 に記載の通信処理装置。

【請求項 3】前記通信処理用リソースは、設定可能なコネクション数を含み、

前記通信処理装置は、

コネクション要求元に対応する利用者識別子と、コネクション数とを対応付け、利用者毎の使用可能なコネクションを設定したリソース使用条件テーブルを有し、

前記制御手段は、

前記利用者識別処理に基づいて識別された利用者に基づいて、リソース使用条件テーブルの検索を実行して、利用可能なコネクションの有無の判別を実行する構成であることを特徴とする請求項 1 に記載の通信処理装置。

【請求項 4】前記制御手段は、

前記利用者識別処理において、コネクション要求の送信元 IP アドレスまたは送信元 MAC アドレスの少なくともいずれかを利用者情報として取得する処理を実行する構成であることを特徴とする請求項 1 に記載の通信処理装置。

【請求項 5】前記制御手段は、

前記利用者識別処理において、コネクション要求の送信先ポート番号を利用者情報として取得し、

取得した送信先ポート番号に対応して設定された通信処理用リソースの空きを確認を条件としてコネクション確立処理を実行する構成を有することを特徴とする請求項 1 に記載の通信処理装置。

【請求項 6】前記制御手段は、

アドレス情報と利用者識別子とを対応付けた利用者テ

2

ブルに基づいてコネクション要求元に対応する利用者を識別する利用者識別処理と、

利用者識別子とリソース領域情報を含むリソース使用条件とを対応付けたリソース使用条件テーブルに基づいて利用者に対応するリソース使用条件を決定するリソース使用条件決定処理と、

リソース領域情報と、リソース空き情報とを対応付けたリソース管理情報テーブルに基づいてコネクション要求利用者に対するコネクション適用リソース領域を設定するリソース領域決定処理と、

を順次実行してコネクション確立処理を実行する構成を有することを特徴とする請求項 1 に記載の通信処理装置。

【請求項 7】前記制御手段は、

アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいてコネクション要求元に対応する利用者を識別する利用者識別処理と、

利用者識別子とリソース領域情報を含むリソース使用条件とを対応付けたリソース使用条件テーブルに基づいて利用者に対応するリソース使用条件を決定するリソース使用条件決定処理と、

リソース領域情報と、リソース空き情報とを対応付けたリソース管理情報テーブルに基づいてコネクション要求利用者に対するコネクション適用リソース領域を設定するリソース領域決定処理と、を順次実行してコネクション確立処理を実行する構成を有し、

前記リソース使用条件テーブルは、優先度の高い利用者の利用者識別子に対するリソース使用条件としてのリソース領域の配分比率を高く設定した構成であることを特徴とする請求項 1 に記載の通信処理装置。

【請求項 8】前記制御手段は、

アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいてコネクション要求元に対応する利用者を識別する利用者識別処理と、

利用者識別子とグループ識別子と、最大コネクション数、および現在のコネクション数とを対応付けたリソース使用条件テーブルに基づいて、前記利用者識別処理によって取得した利用者識別データに基づく該リソース使用条件テーブルのエントリ検索により、利用可能なコネクションの有無を判定してリソース使用可否を判定するリソース使用条件決定処理と、

を順次実行してコネクション確立処理を実行する構成を有することを特徴とする請求項 1 に記載の通信処理装置。

【請求項 9】前記制御手段は、

アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいてコネクション要求元に対応する利用者を識別する利用者識別処理と、

利用者識別子とグループ識別子と、最大コネクション数、および現在のコネクション数とを対応付けたリソ

ス使用条件テーブルに基づいて、前記利用者識別処理によって取得した利用者識別データに基づく該リソース使用条件テーブルのエントリ検索により、利用可能な接続の有無を判定してリソース使用可否を判定するリソース使用条件決定処理とを順次実行して接続確立処理を実行する構成を有し、

前記リソース使用条件テーブルは、優先度の高い利用者の利用者識別子を複数の異なるグループ識別子に対応付けて格納した構成であることを特徴とする請求項 1 に記載の通信処理装置。

【請求項 10】前記制御手段は、接続要求として TCP 接続要求に含まれる SYN パケットの受信に応じて、接続確立可否の決定処理を実行する構成であり、SYN パケットに含まれる送信元識別データに基づいて利用者の識別を実行する構成であることを特徴とする請求項 1 に記載の通信処理装置。

【請求項 11】通信接続要求を受信し、接続確立処理を実行する通信処理方法において、接続要求データに基づいて、接続要求元に対応する利用者の識別処理を実行する利用者識別処理ステップと、

前記利用者識別処理において識別された利用者識別子に対応して設定された通信処理用リソースの空きを確認を条件として接続確立処理を実行するリソース決定処理ステップと、を有することを特徴とする通信処理方法。

【請求項 12】前記通信処理方法において、前記通信処理用リソースは、複数の領域に分割されたメモリまたは記憶装置の記憶領域を含み、前記リソース決定処理ステップは、前記利用者識別処理に基づいて識別された利用者に基づいて、接続要求元に対応する利用者識別子と、前記記憶領域の各々とを対応付け、利用者毎の使用可能な記憶領域を設定したリソース使用条件テーブルの検索を実行して、利用可能なリソースとしての記憶領域の判別を実行するステップを含むことを特徴とする請求項 11 に記載の通信処理方法。

【請求項 13】前記通信処理方法において、前記通信処理用リソースは、設定可能な接続数を含み、前記リソース決定処理ステップは、前記利用者識別処理に基づいて識別された利用者に基づいて、接続要求元に対応する利用者識別子と、接続数とを対応付け、利用者毎の使用可能な接続を設定したリソース使用条件テーブルの検索を実行して、利用可能な接続の有無の判別を実行するステップを含むことを特徴とする請求項 11 に記載の通

信処理方法。

【請求項 14】前記利用者識別処理ステップは、接続要求の送信元 IP アドレスまたは送信元 MAC アドレスの少なくともいずれかを利用者情報として取得する処理を実行することを特徴とする請求項 11 に記載の通信処理方法。

【請求項 15】前記利用者識別処理ステップは、接続要求の送信先ポート番号を利用者情報として取得し、

10 前記リソース決定処理ステップは、取得した送信先ポート番号に対応して設定された通信処理用リソースの空きを確認を条件として接続確立処理を実行することを特徴とする請求項 11 に記載の通信処理方法。

【請求項 16】前記通信処理方法は、アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいて接続要求元に対応する利用者を識別する利用者識別処理ステップと、利用者識別子とリソース領域情報を含むリソース使用条件とを対応付けたリソース使用条件テーブルに基づいて利用者に対応するリソース使用条件を決定するリソース使用条件決定処理ステップと、リソース領域情報と、リソース空き情報とを対応付けたリソース管理情報テーブルに基づいて接続要求利用者に対する接続適用リソース領域を設定するリソース領域決定処理ステップと、を順次実行して接続確立処理を実行することを特徴とする請求項 11 に記載の通信処理方法。

【請求項 17】前記通信処理方法は、
30 アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいて接続要求元に対応する利用者を識別する利用者識別処理ステップと、利用者識別子とグループ識別子と、最大接続数、および現在の接続数とを対応付けたリソース使用条件テーブルに基づいて、前記利用者識別処理によって取得した利用者識別データに基づく該リソース使用条件テーブルのエントリ検索により、利用可能な接続の有無を判定してリソース使用可否を判定するリソース使用条件決定処理ステップと、
40 を順次実行して接続確立処理を実行することを特徴とする請求項 11 に記載の通信処理方法。

【請求項 18】前記利用者識別処理ステップは、接続要求として TCP 接続要求に含まれる SYN パケットの受信に応じて、SYN パケットに含まれる送信元識別データに基づいて利用者の識別を実行するステップを含むことを特徴とする請求項 11 に記載の通信処理方法。

【請求項 19】通信接続要求を受信し、接続確立処理を実行する通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであ

って、
 コネクション要求データに基づいて、コネクション要求元に対応する利用者の識別処理を実行する利用者識別処理ステップと、
 前記利用者識別処理において識別された利用者識別子に対応して設定された通信処理用リソースの空きの確認を条件としてコネクション確立処理を実行するリソース決定処理ステップと、
 を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信処理装置、および通信処理方法、並びにコンピュータ・プログラムに関する。詳細には、ネットワークに接続されたサーバ等における例えばTCPを用いた通信コネクション処理において、サーバで使用可能なコネクション処理用のリソース量を通信相手に応じて制限することにより、優先度の高い通信相手との通信を優先度の低い通信相手との通信によって妨げられることを防止した通信処理装置、および通信処理方法、並びにコンピュータ・プログラムに関する。

【0002】

【従来の技術】インターネット回線の高速化及び常時接続の普及により、個人が自宅でPCをインターネットに常時接続しサーバとして使用することが可能となりつつある。例えばこのような自宅のPCをサーバとして使用する場合はサーバの利用者を想定すると、家庭内のサーバ利用者は、主に次の3種類の対象が存在する。

サーバ所有者

サーバ所有者の家族、友人

上記以外の不特定な対象

【0003】特に、現在は、日記やWebページ、デジタル写真画像、自分の作成した映像、音声データをインターネットで一般に公開したいという要望は高まってきており、個人のサーバにおいても不特定な利用者からのアクセスは十分想定される。ここで個人のサーバにおける要求として、サービス使用に対して優先度を設定したいという要求が存在する。基本的に所有者の利用が第一に優先され、不特定な利用者のサービス使用により所有者のサービス使用が妨害を受けることは避けられることが要求される。

【0004】しかしながら、従来のサーバではサービスに使われるTCPコネクション確立の際に、利用者に応じて優先度を設定するような機能は存在していない。TCPトラフィック処理用のリソース（メモリ領域、ディスク領域）は一定量確保されており、TCPコネクション及びコネクション要求の処理時に利用者は考慮されず、同じリソースが制限なく使用されている。

【0005】このため、個人のサーバのように利用者に対して優先度を設定することが望まれる環境では、TCP

Pトラフィック処理用のリソースが優先度の低い利用者により使い切られてしまうと、優先度の高い利用者がサーバを使用できなくなるという問題がある。優先度の低い利用者によりTCPトラフィック処理用のリソースが使い切られるのは次の2つの場合である。

【0006】（ケース1）優先度の低い複数の利用者により、多量のTCPコネクションが確立された場合。

（ケース2）優先度の低い利用者から、TCPトラフィック処理用のリソースに対するDoS（denial of service）攻撃が行われた場合。DoS攻撃は正当な使用者が使用するはずのリソースを、不正な使用者が使い切る、もしくはリソースを使えない状態にすることで、正当な使用者によるリソース使用を妨げるハッキング行為である。例えば大量のデータや不正パケットを送り付けたり、OSやアプリケーションのバグを利用して不正なコマンドを送ることによってシステムをダウンさせる攻撃である。

【0007】TCPトラフィック処理用のリソースに対するDoS攻撃としては、主に次の2つが挙げられる。

・SYN Flood攻撃

・TCPコネクションを大量に確立するDoS攻撃

【0008】SYN Flood攻撃は、TCP/IPでコネクションを確立するために行われる3ウェイハンドシェイクプロトコルにおいて確立途中の状態を管理するキューのデータサイズが有限であることを利用した攻撃である。ターゲットサーバにTCPコネクションの確立を要求するSYNパケットを大量に送り、3ウェイハンドシェイクプロトコルを終了しないことで確立途中の状態を大量に作る。この攻撃によりターゲットサーバの確立途中の状態を管理するキューが溢れ、新たなTCPコネクションを確立することを一時的に不可能にする。

【0009】TCPコネクションを大量に作るというDoS攻撃の概要を以下説明する。TCPコネクションが確立される度にメモリ、CPUなどのリソースが使用されるため、一度に処理可能なTCPコネクション数には上限が存在する。そこでターゲットサーバに対し複数のマシンを用いて大量のTCPコネクションを確立し、上限までリソースを使い切ってしまうと、ターゲットサーバは新たなTCPコネクションを確立不能になる。ターゲットサーバの能力によっては処理速度の低下やシステムの停止といった現象が起こる。

【0010】従来のDoS攻撃に対する防御策として、ファイアウォール（Firewall）やルータ（Router）を用いてフィルタリングを行う方法がある。これらのフィルタリング方法ではTCPコネクションの確立の際に送信元IPアドレス、使用ポートに関し制限を行うことが可能であり、条件を満たさないTCPコネクション要求は廃棄される。

【0011】フィルタリングを使用することによりサーバの利用者に対して使用するサービスを限定することが

でき、利用の許可されていない不正な利用者からのDOS攻撃を防ぐことができる。しかしながら、サービスの使用が許可されている利用者間では、サーバのTCPコネクションリソースの使用権限に差がないため、上記した(ケース1)、(ケース2)の場合をどちらも防ぐことができない。

【0012】また、SYN Flood攻撃に対する防御策に関しては、“SYN cookies”という方法が存在する。これはLinuxOSのkernel version 2.0.30以降でオプションとしてつけられた機能である。

従来のTCPコネクション要求処理では、要求であるSYNパケット受信時に、コネクションに対するリソースが確保されるが、SYN cookiesでは、リソースを確保せずにSYNパケットへの応答であるSYN-ACKパケットを返し、ACKパケットを受けとりコネクションが確立された時点で初めてリソースを確保する。この方法によりSYN Flood攻撃を防ぐ。

【0013】この手法では、上記の(ケース2)におけるSYN Flood攻撃を防ぐことができるが、従来のTCPトラフィック処理と同様に利用者の優先度を区別する仕組みがないため、(ケース1)及び(ケース2)におけるTCPコネクションを多量に確立することによるDOS攻撃の場合には、優先度の低い利用者のTCPコネクションによりリソースが使い切られてしまう。

【0014】また、SYN Flood攻撃に対する別の防御手段としてMicrosoft社がWindowsNT4.0SP2以降に導入した方法が存在する。これは、SYN Flood攻撃により確立途中のTCPコネクションの状態を管理するキューが溢れた際に、キューのサイズの増加、タイムアウト時間設定値の減少などの防衛手段を行う。この方法もSYN Flood攻撃を効きにくくする効果はあるが、“SYN cookies”と同様に(ケース1)及び(ケース2)におけるTCPコネクションを多量に確立することによるDOS攻撃の場合には、優先度の低い利用者のTCPコネクションによりリソースが使い切られてしまうという問題が発生する。

【0015】

【発明が解決しようとする課題】個人のサーバのように利用者に対して優先度を設定することが望まれる環境では、TCPトラフィック処理用のリソースが優先度の低い利用者により使い切られてしまうと、優先度の高い利用者がサーバを使用できなくなるという問題がある。問題が生じるのは、上述した次の2つの場合である。

(ケース1) 複数の優先度の低い利用者により、多量のTCPコネクションが確立された場合。

(ケース2) 優先度の低い利用者から、TCPトラフィック処理用のリソースに対するDOS攻撃が行われた場合。

【0016】この2つの場合にも優先度の高い利用者が

TCPコネクションを確立し、サーバを使用できるようにすることが必要である。

【0017】本発明は、上述の問題点を解決することを目的とするものであり、上述の(ケース1)、(ケース2)のような場合にも、優先度の高い利用者がTCPコネクションを確立し、サーバを使用できるようにすることを可能とする通信処理装置、および通信処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

10 【0018】

【課題を解決するための手段】本発明の第1の側面は、通信コネクション要求を受信し、コネクション確立処理を実行する通信処理装置において、コネクション要求に対するコネクション確立可否の決定処理を実行する制御手段を有し、前記制御手段は、コネクション要求データに基づいて、コネクション要求元に対応する利用者の識別処理を実行し、該利用者識別処理において識別された利用者識別子に対応して設定された通信処理用リソースの空きを確認を条件としてコネクション確立処理を実行する構成を有することを特徴とする通信処理装置にある。

20

【0019】さらに、本発明の通信処理装置の一実施態様において、前記通信処理用リソースは、複数の領域に分割されたメモリまたは記憶装置の記憶領域を含み、前記通信処理装置は、コネクション要求元に対応する利用者識別子と、前記記憶領域の各々を対応付け、利用者毎の使用可能な記憶領域を設定したリソース使用条件テーブルを有し、前記制御手段は、前記利用者識別処理に基づいて識別された利用者に基づいて、リソース使用条件テーブルの検索を実行して、利用可能なリソースとしての記憶領域の判別を実行する構成であることを特徴とする。

30

【0020】さらに、本発明の通信処理装置の一実施態様において、前記通信処理用リソースは、設定可能なコネクション数を含み、前記通信処理装置は、コネクション要求元に対応する利用者識別子と、コネクション数とを対応付け、利用者毎の使用可能なコネクションを設定したリソース使用条件テーブルを有し、前記制御手段は、前記利用者識別処理に基づいて識別された利用者に基づいて、リソース使用条件テーブルの検索を実行して、利用可能なコネクションの有無の判別を実行する構成であることを特徴とする。

40

【0021】さらに、本発明の通信処理装置の一実施態様において、前記制御手段は、前記利用者識別処理において、コネクション要求の送信元IPアドレスまたは送信元MACアドレスの少なくともいずれかを利用者情報として取得する処理を実行する構成であることを特徴とする。

【0022】さらに、本発明の通信処理装置の一実施態様において、前記制御手段は、前記利用者識別処理にお

50

いて、コネクション要求の送信先ポート番号を利用者情報として取得し、取得した送信先ポート番号に対応して設定された通信処理用リソースの空きを確認を条件としてコネクション確立処理を実行する構成を有することを特徴とする。

【0023】さらに、本発明の通信処理装置の一実施態様において、前記制御手段は、アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいてコネクション要求元に対応する利用者を識別する利用者識別処理と、利用者識別子とリソース領域情報を含むリソース使用条件とを対応付けたリソース使用条件テーブルに基づいて利用者に対応するリソース使用条件を決定するリソース使用条件決定処理と、リソース領域情報と、リソース空き情報とを対応付けたリソース管理情報テーブルに基づいてコネクション要求利用者に対するコネクション適用リソース領域を設定するリソース領域決定処理と、を順次実行してコネクション確立処理を実行する構成を有することを特徴とする。

【0024】さらに、本発明の通信処理装置の一実施態様において、前記制御手段は、アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいてコネクション要求元に対応する利用者を識別する利用者識別処理と、利用者識別子とリソース領域情報を含むリソース使用条件とを対応付けたリソース使用条件テーブルに基づいて利用者に対応するリソース使用条件を決定するリソース使用条件決定処理と、リソース領域情報と、リソース空き情報とを対応付けたリソース管理情報テーブルに基づいてコネクション要求利用者に対するコネクション適用リソース領域を設定するリソース領域決定処理と、を順次実行してコネクション確立処理を実行する構成を有し、前記リソース使用条件テーブルは、優先度の高い利用者の利用者識別子に対するリソース使用条件としてのリソース領域の配分比率を高く設定した構成であることを特徴とする。

【0025】さらに、本発明の通信処理装置の一実施態様において、前記制御手段は、アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいてコネクション要求元に対応する利用者を識別する利用者識別処理と、利用者識別子とグループ識別子と、最大コネクション数、および現在のコネクション数とを対応付けたリソース使用条件テーブルに基づいて、前記利用者識別処理によって取得した利用者識別データに基づく該リソース使用条件テーブルのエントリ検索により、利用可能なコネクションの有無を判定してリソース使用可否を判定するリソース使用条件決定処理と、を順次実行してコネクション確立処理を実行する構成を有することを特徴とする。

【0026】さらに、本発明の通信処理装置の一実施態様において、前記制御手段は、アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいてコネクシ

ョン要求元に対応する利用者を識別する利用者識別処理と、利用者識別子とグループ識別子と、最大コネクション数、および現在のコネクション数とを対応付けたリソース使用条件テーブルに基づいて、前記利用者識別処理によって取得した利用者識別データに基づく該リソース使用条件テーブルのエントリ検索により、利用可能なコネクションの有無を判定してリソース使用可否を判定するリソース使用条件決定処理とを順次実行してコネクション確立処理を実行する構成を有し、前記リソース使用条件テーブルは、優先度の高い利用者の利用者識別子を複数の異なるグループ識別子に対応付けて格納した構成であることを特徴とする。

【0027】さらに、本発明の通信処理装置の一実施態様において、前記制御手段は、コネクション要求としてTCPコネクション要求に含まれるSYNパケットの受信に応じて、コネクション確立可否の決定処理を実行する構成であり、SYNパケットに含まれる送信元識別データに基づいて利用者の識別を実行する構成であることを特徴とする。

【0028】さらに、本発明の第2の側面は、通信コネクション要求を受信し、コネクション確立処理を実行する通信処理方法において、コネクション要求データに基づいて、コネクション要求元に対応する利用者の識別処理を実行する利用者識別処理ステップと、前記利用者識別処理において識別された利用者識別子に対応して設定された通信処理用リソースの空きを確認を条件としてコネクション確立処理を実行するリソース決定処理ステップと、を有することを特徴とする通信処理方法にある。

【0029】さらに、本発明の通信処理方法の一実施態様において、前記通信処理方法において、前記通信処理用リソースは、複数の領域に分割されたメモリまたは記憶装置の記憶領域を含み、前記リソース決定処理ステップは、前記利用者識別処理に基づいて識別された利用者に基づいて、コネクション要求元に対応する利用者識別子と、前記記憶領域の各々とを対応付け、利用者毎の使用可能な記憶領域を設定したリソース使用条件テーブルの検索を実行して、利用可能なリソースとしての記憶領域の判別を実行するステップを含むことを特徴とする。

【0030】さらに、本発明の通信処理方法の一実施態様において、前記通信処理方法において、前記通信処理用リソースは、設定可能なコネクション数を含み、前記リソース決定処理ステップは、前記利用者識別処理に基づいて識別された利用者に基づいて、コネクション要求元に対応する利用者識別子と、コネクション数とを対応付け、利用者毎の使用可能なコネクションを設定したリソース使用条件テーブルの検索を実行して、利用可能なコネクションの有無の判別を実行するステップを含むことを特徴とする。

【0031】さらに、本発明の通信処理方法の一実施態様において、前記利用者識別処理ステップは、コネクシ

ョン要求の送信元 I P アドレスまたは送信元 M A C アドレスの少なくともいずれかを利用者情報として取得する処理を実行することを特徴とする。

【0032】さらに、本発明の通信処理方法の一実施態様において、前記利用者識別処理ステップは、コネクション要求の送信先ポート番号を利用者情報として取得し、前記リソース決定処理ステップは、取得した送信先ポート番号に対応して設定された通信処理用リソースの空きを確認を条件としてコネクション確立処理を実行することを特徴とする。

【0033】さらに、本発明の通信処理方法の一実施態様において、前記通信処理方法は、アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいてコネクション要求元に対応する利用者を識別する利用者識別処理ステップと、利用者識別子とリソース領域情報を含むリソース使用条件とを対応付けたリソース使用条件テーブルに基づいて利用者に対応するリソース使用条件を決定するリソース使用条件決定処理ステップと、リソース領域情報と、リソース空き情報とを対応付けたリソース管理情報テーブルに基づいてコネクション要求利用者に対するコネクション適用リソース領域を設定するリソース領域決定処理ステップと、を順次実行してコネクション確立処理を実行することを特徴とする。

【0034】さらに、本発明の通信処理方法の一実施態様において、前記通信処理方法は、アドレス情報と利用者識別子とを対応付けた利用者テーブルに基づいてコネクション要求元に対応する利用者を識別する利用者識別処理ステップと、利用者識別子とグループ識別子と、最大コネクション数、および現在のコネクション数とを対応付けたリソース使用条件テーブルに基づいて、前記利用者識別処理によって取得した利用者識別データに基づく該リソース使用条件テーブルのエントリ検索により、利用可能なコネクションの有無を判定してリソース使用可否を判定するリソース使用条件決定処理ステップと、を順次実行してコネクション確立処理を実行することを特徴とする。

【0035】さらに、本発明の通信処理方法の一実施態様において、前記利用者識別処理ステップは、コネクション要求として T C P コネクション要求に含まれる S Y N パケットの受信に応じて、S Y N パケットに含まれる送信元識別データに基づいて利用者の識別を実行するステップを含むことを特徴とする。

【0036】さらに、本発明の第3の側面は、通信コネクション要求を受信し、コネクション確立処理を実行する通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、コネクション要求データに基づいて、コネクション要求元に対応する利用者の識別処理を実行する利用者識別処理ステップと、前記利用者識別処理において識別された利用者識別子に対応して設定された通信処理用リソースの空きを確認を条

件としてコネクション確立処理を実行するリソース決定処理ステップと、を有することを特徴とするコンピュータ・プログラムにある。

【0037】なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、C D や F D、M O などの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0038】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0039】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施態様の詳細について説明する。

【0040】ネットワーク端末における T C P コネクションに関する処理の概略について、図1を参照して説明する。

【0041】物理ネットワークは、O S I 参照モデルの第1層に相当し、電気信号や光信号によるデータ送受信の確立、コネクタ、ケーブル等のデータ伝送路における処理を行なう。ネットワークインタフェース層処理は、O S I 参照モデル第2層に相当し、通信機器間でのパケットの認識、送受信処理を行なう。インターネット層は、O S I 参照モデル第3層に相当し、アドレス管理および伝送経路の選択処理を行なう。トランスポート層処理は、O S I 参照モデル第4層に相当し、通信機器間のデータ転送制御と、データ転送の信頼性確率処理を行なう。アプリケーション層処理は、O S I 参照モデル第7層に相当し、アプリケーションが送受信を行なうための通信処理制御や、アプリケーションの固有処理の対応を行なう。

【0042】本発明は図1におけるトランスポート層処理内に存在する T C P コネクション処理手法の改善に関するものであり、従来の T C P コネクション処理手法に加え、次の手段を具備する。

【0043】・ T C P コネクション要求トラフィックデータから利用者を識別する手段

・各利用者のリソース使用条件を取得する手段

・各利用者に対しリソース使用条件を考慮し使用可能なリソースの有無を確認する手段

・現在のリソースの使用状況を管理する手段

・各利用者のリソース使用条件を設定する手段

【0044】なお、上記記載において、利用者とは、通

信処理装置に対して接続要求を行ってきた通信要求者、あるいは通信要求端末であり、リソースとは、TCPトラフィック処理用のリソース（メモリ領域、ディスク領域）のことである。

【0045】本発明の通信処理装置は、予め利用者、すなわち通信要求者、あるいは通信要求端末毎のリソース使用条件の設定情報を通信処理装置内に有し、通信要求を受信した場合に、リソース使用条件設定情報に従って、設定された条件の下でのリソースを使用した通信が可能か否かを判定して、可能な場合のみ設定条件の下でのリソース処理を行なって通信を実行する。

【0046】図2に通信装置間で送受信される通信パケットの構成例として、IPパケットのTCP(Transmission Control protocol)フォーマットを示す。TCPヘッダには、送信元ポート番号、宛先ポート番号、データパケットの先頭がそのデータの送信初めから何バイトにあたるかをバイト数で示したデータ順序を示すシーケンス番号、相手から次に送られるデータの送信シーケンス番号を示す受信確認番号、ヘッダ長、TCPセグメントの処理方法などのコードビットからなるヘッダ情報、データの残り受信可能バイト数を示すウィンドウサイズ、TCPパケットの信頼性保証値としてのチェックサム、緊急処理を要するデータを示す緊急ポインタを有する。

【0047】次に、図3にIPパケット構成のIPヘッダの詳細を示す。IPv4、IPv6等のバージョンを示すバージョン、ヘッダ長、さらに、優先度情報を格納したTOS(Type of Service)フィールド、パケットの長さ、パケットの識別子、IP層でのデータ分割（フラグメント）に関する制御情報としてのフラグ、分割（フラグメント）されたデータの場所を示す断片オフセット、データの破棄までの時間情報を示すTTL(Time to Live)、上位層で利用されるプロトコル（4:IP, TCP:7, UDP:17...）ヘッダのチェックサム、送信元IPアドレス、宛て先IPアドレスを有する。

【0048】本発明の通信処理装置によるTCPコネクション要求受信時の処理の流れを図4のフローチャートを参照して説明する。

【0049】通信処理装置は、ステップS01において、TCPコネクション要求のトラフィックデータを受信する。TCPでは、コネクション確立時にSYNパケット、SYNACK、ACKの送受信を3ウェイハンドシェイク制御メッセージ交換処理として実行する。この際のトラフィックデータはSYNパケットの内容、SYNパケットの含まれていたフレーム（パケット）のフレームヘッダ、データグラムヘッダである。

【0050】通信処理装置は、ステップS02において、受信したトラフィックデータとしてのフレーム（パケット）を解析して利用者を識別する。利用者識別処理

としては、例えば送信元MACアドレス、送信元IPアドレス、送信元ポート番号、送信先ポート番号の各値に関する条件の組み合わせを取得する処理として実行される。

【0051】次にステップS03において、利用者に対するリソース使用条件を取得する。利用者に対するリソース使用条件は、通信処理装置において、利用者に対応付けて予め設定された条件であり、この具体例については後述する。ステップS04において、取得したリソース使用条件とリソースの使用状況を元に現在使用可能なリソースが存在するか確認する。現在使用可能なリソースが存在する場合（S05においてYes）には、リソースの使用状況を変更し（ステップS06）、通常のTCPコネクション要求処理を行う（ステップS07）。使用可能なリソースが存在しない場合（S05においてNo）は、このTCPコネクション要求を棄却する。

（ステップS08）

【0052】また、3ウェイハンドシェイク途中のタイムアウト及び、コネクションの終了時などTCPコネクション要求処理以外のTCPコネクション処理においてリソースが開放される場合には、リソース開放後にリソースの使用状況の変更処理を行う。

【0053】本構成により、利用者に応じてリソースの使用条件の設定を行うことが可能となり、優先度の低い利用者の使用可能なリソース量を制限することが可能となる。

【0054】優先度の低い利用者の使用可能なリソースを制限することで、優先度の低い利用者がTCPコネクション処理に関わる全リソースを使い切ることが防止されるとともに、優先度の高い利用者専用のリソースを確保することが可能となるため、優先度の低い利用者によりサーバが混んでいる際にも、優先度の高い利用者は優先的に効率的にサーバを利用することができる。

【0055】優先度の低い利用者は、TCPコネクションに関するDOS攻撃により優先度の低い利用者に対してサービス利用を妨害することは可能であるが、攻撃が行われている間でも優先度の高い利用者は、優先度の低い利用者が使用できないリソースを使用してサービスを利用することが可能であり（前述したケース2）の問題を解決することが可能である。

【0056】また、同様に優先度の低い利用者による多量のアクセスが発生してサービス使用の効率が落ちている場合であっても、優先度の高い利用者は専用のリソースを使用することでサービスを優先的に使用することが可能であり（前述したケース1）の問題を解決することが可能である。

【0057】優先度に応じて利用者毎にリソースを割り当てる具体的構成例について以下、リソース決定処理例1およびリソース決定処理例2として説明する。リソース決定処理例1はリソースを複数の領域に分けて管理し

利用者ごとに使用可能なリソース領域を制限して、制限領域の使用状況に応じて優先度に応じた利用者毎の接続の設定可否を判定する方法である。リソース決定処理例 2 は、利用者ごとに接続数を制限して、優先度に応じた利用者毎の接続の設定可否を判定する方法である。

【0058】[リソース決定処理例 1]従来の TCP 接続処理では、使用するリソース、すなわち、TCP トラフィック処理用のリソース（メモリ領域、ディスク領域）は利用者、すなわち通信相手となる通信要求者、あるいは通信要求端末によらず、一定の領域内で使用される。以下に説明する本発明の通信処理装置におけるリソース決定処理例 1 は、これを改良し、リソースを複数の領域に分けて管理し、利用者に対しリソース領域ごとに使用制限を与える。

【0059】本発明の通信処理装置は、従来の TCP 接続処理に加えて、次の処理を実行する。すなわち以下の処理を実行する機能拡張された構成を持つ。

- ・TCP 接続処理に用いるリソースの複数の領域への分割
- ・TCP 接続処理において接続ごとの使用リソース領域の指定
- ・TCP 接続要求処理の直前へのリソース決定処理の追加

【0060】この機能拡張により、接続ごとに利用者を識別して、利用者に応じたリソース領域を指定した TCP 接続が可能となる。本発明の通信処理装置は、TCP 接続処理に用いるリソースを複数の領域へ分割した構成を持ち、図 1 に示した TCP 接続処理中のトランスポート層処理内の処理として、接続要求に応じて、接続ごとの利用者を判別して使用リソース領域の決定処理を行なう。

【0061】リソース決定処理は、3つのフェーズによって構成される。第 1 フェーズは、TCP 接続要求のトラフィックデータの情報から利用者を識別、または利用者及び利用するサービスの双方を識別する利用者識別処理、第 2 フェーズは、識別された利用者に応じて、リソースの使用条件を与えるリソース使用条件決定処理、第 3 フェーズは、リソース使用条件から使用するリソース領域を決定するリソース領域決定処理、である。この 3 フェーズからなるリソース決定処理により、利用者に応じてリソース領域の使用を制限することが可能となる。

【0062】図 5 に、本発明の通信処理装置に対する TCP 接続要求に対して、通信処理装置において通信処理制御を実行する制御手段の実行するリソース決定処理の詳細を説明する図を示す。

【0063】TCP 接続処理用リソース 150 は、TCP トラフィック処理用のリソース（メモリ領

域、ディスク領域）をまとめて示している。リソース 150 は、図に示すように複数の領域 1〜N に分割されている。

【0064】図 6 に本発明の通信処理装置における TCP 接続要求に対して実行されるリソース決定処理の概略を説明するフローを示す。TCP 接続要求、すなわち 3 ウェイハンドシェイクプロトコルに従った SYN パケットを受信すると、リソース決定処理部 130 において、上述した 3 つのフェーズの処理が実行される。

【0065】図 6 のステップ S11 において、TCP 接続要求のトラフィックデータの情報から利用者を識別、または利用者及び利用するサービスの双方を識別する利用者識別処理が実行され、次にステップ S12 において、識別された利用者に応じて、リソースの使用条件を与えるリソース使用条件決定処理が実行され、次に、ステップ S13 において、リソース使用条件から使用するリソース領域を決定するリソース領域決定処理が実行され、リソースの使用の可否判定に基づいて TCP 接続要求に対する応答を行なう。すなわちリソース使用可能であり通信接続を設定可能な状態（S14 で Yes）であれば、SYNACK パケットの送信を実行し、リソース使用不可の場合（S14 で No）には、受信 SYN パケットの破棄（S15）を実行する。

【0066】図 5 に示すように、3つのフェーズの処理、すなわち、利用者識別処理、リソース使用条件決定処理、リソース領域決定処理において、記憶装置 140 に記憶された各テーブル、すなわち利用者テーブル 111、リソース使用条件テーブル 112、リソース管理情報テーブル 113 を参照した処理が実行される。これらの各テーブルに対する情報格納、更新処理は、それぞれ利用者設定処理部 121、リソース使用条件設定処理部 122、リソース管理情報設定処理部 123 が行なう。

【0067】以下、各テーブル構成例を図面に示し、図を参照しながらリソース決定処理部 130 におけるリソース決定処理の各フェーズにおける処理の詳細について説明する。

【0068】（フェーズ 1：利用者識別処理）利用者識別処理は、通信処理装置が受信した SYN パケットから利用者、すなわち通信処理装置に対して接続要求を行ってきた通信要求者、あるいは通信要求端末を識別する処理である。この利用者識別処理は、利用者テーブル 111 を参照した処理として実行される。

【0069】利用者テーブルの構成例を図 7 に示し、利用者テーブルを参照した利用者識別処理の処理フローを図 8 に示す。利用者テーブルは、図 7 に示すように、利用者 ID、送信元 MAC アドレス、送信元 IP アドレス、送信先ポート番号の各フィールドを有する。

【0070】図 7 に示す利用者テーブルでは、空欄は任

意の値が可能であることを表している。各利用者IDに対して1つまたは複数の識別条件を設定できる。例えば図7の例では、SYNパケットの送信元MACアドレスが35.42.1.56.1375または送信元IPアドレスが45.87.123.245であれば利用者IDは所有ユーザであると識別する。

【0071】また、送信元IPアドレスが42.134.78.95であれば利用者IDは友人Aであると識別する。その他の送信元MACアドレス、送信元IPアドレスが受信SYNパケットから得られた場合は、一般、すなわち所有ユーザおよび友人A以外からのコネクション要求であると判定することができる。

【0072】利用者テーブルを参照した利用者識別処理の詳細を図8のフローチャートを参照して説明する。

【0073】通信処理装置は、まず、TCPコネクション要求として受け取ったSYNパケットから送信元IPアドレス、送信先ポート番号を抽出する。(ステップS21)。これらの情報は、SYNパケットのIPヘッダ(図3参照)、TCPヘッダ(図2参照)から取得可能である。次にこのSYNパケットのフレームヘッダを得ることができれば送信元MACアドレスを抽出する。

(ステップS22)。これらの抽出した情報を用いて利用者テーブルを検索し(ステップS23)、利用者IDを取得し、次のリソース使用条件決定処理に渡す(ステップS24、S25)。利用者テーブルから利用者IDが取得できなかった場合は、ステップS26で「null」を結果として、次のリソース使用条件決定処理に渡す。

【0074】(フェーズ2:リソース使用条件決定処理)リソース使用条件決定処理は、上述した利用者識別処理において識別された利用者に応じて、リソース使用条件を決定する処理である。このリソース使用条件決定処理は、リソース使用条件決定テーブル112を参照した処理として実行される。

【0075】リソース使用条件決定テーブルの構成例を図9に示し、リソース使用条件決定テーブルを参照したリソース使用条件決定処理の処理フローを図10に示す。リソース使用条件決定テーブルは、図9に示すように、利用者IDに対して、リソース使用条件としての使用可能なリソース領域番号を対応付けたテーブルとして構成される。テーブルのリソース使用条件フィールドには、各利用者IDに対応して利用可能なリソース領域番号が格納され、後述するフェーズ3のリソース領域決定処理において、空き領域を探索する順番に領域番号がシャッフルに並べられて格納される。例えばユーザID=Aの利用可能なリソース領域番号が、1, 2, 3, 4, 7であり、領域探索の指定順序も1, 2, 3, 4, 7の順である場合、テーブルのリソース使用条件フィールドには、1, 2-4, 7のようにデータが格納される。

【0076】図9に示すテーブル例では、上述の利用者識別処理において取得された利用者IDが、例えば所有ユーザ1であった場合は、使用可能なリソース領域は1~9の領域であることを示し、友人Aである場合は、使用可能なリソース領域は3~9の領域、一般である場合は、8~9の領域、その他、すなわち「null」である場合は、9のリソース領域のみが使用可能であることを示している。すなわち、上述の利用者識別処理において取得された利用者IDに基づいて、リソース使用条件決定テーブルから使用可能なリソース領域番号を取得する処理が、リソース使用条件決定処理として実行される。

【0077】図10を参照して、リソース使用条件決定処理の処理について説明する。リソース使用条件決定処理は、前述のフェーズ1の利用者識別処理の結果を取得して実行される。利用者識別処理の結果として、利用者IDを受け取り、その値でリソース使用条件テーブルを検索する。(ステップS31)。この検索処理において、利用者IDに対応するエントリがあれば(S32でYes)エントリのリソース使用条件を次のリソース領域決定処理に渡す(ステップS33)。対応するエントリがない場合(S32でNo)には「null」を結果として渡す(ステップS34)。

【0078】(フェーズ3:リソース領域決定処理)リソース領域決定処理は、上述したリソース使用条件決定処理において決定されたリソース使用条件に応じて、空き領域があるリソース領域を探し、使用するリソースを決定する処理である。このリソース領域決定処理は、リソース管理情報テーブル113を参照した処理として実行される。

【0079】リソース管理情報テーブルの構成例を図11に示し、リソース管理情報テーブルを参照したリソース領域決定処理の処理フローを図12に示す。リソース管理情報テーブルは、図11に示すように、リソース領域番号、最大コネクション数、受信キューサイズ、空き領域の有無、リソース領域開始アドレスの各データを対応付けたテーブルである。

【0080】リソース管理情報テーブルでは、リソース領域はリソース領域番号により識別される。最大コネクション数はリソース領域で管理可能なTCPコネクション数である。受信キューサイズは、3ウェイハンドシェイクプロトコルが終了していないコネクション確立途中の状態の保持可能な個数である。この図11に示す例は、この2つの数値、すなわち、リソース領域で管理可能なTCPコネクション数と、3ウェイハンドシェイクプロトコルが終了していないコネクション確立途中のコネクション待機数とにより各リソース領域を区分し、リソース領域のサイズを決定する構成としたテーブル例であるが、これらの構成に限らず、例えばコネクション数、キューサイズに関して、バイト数または全リソース

中に占める割合を設定値として、これらの設定値に基づいて、領域の区分を行なう構成としてもよい。

【0081】空き領域の有無はリソース領域にコネクション要求を処理できる空き領域が存在するか否かを表す。この値はTCPコネクション処理において、コネクション数または確立途中のコネクション用のキューが一杯になった時に「無」に変更され、空きができた際に「有」に変更され、コネクション状態に応じて、逐次、更新される。リソース領域開始アドレスはTCPコネクション処理がリソース領域を使うために使用するアドレスであり、メモリ領域、ディスク領域のポインタに対応する。

【0082】リソース領域決定処理は、図11に示すようなリソース管理情報テーブルを使用して、利用者識別処理、およびリソース使用条件決定処理において決定されたリソース選択条件の順番で、空き領域があるリソース領域を探し、使用するリソースを決定する。

【0083】リソース領域決定処理の流れを図12に示すフローチャートを参照して説明する。リソース領域決定処理は、前述のフェーズ2のリソース使用条件決定処理の結果を取得して実行される。まず、ステップS41において、リソース使用条件決定処理の結果であるリソース使用条件として、前述のリソース使用条件テーブルから選択されたリソース領域番号を取得する。ステップS42では、取得したリソース領域番号にしたがって、順番に使用可能なリソース領域に空き領域があるかをリソース管理情報テーブルを用いて探索する。

【0084】例えばリソース使用条件決定処理の結果であるリソース使用条件として、前述のリソース使用条件テーブルから選択されたリソース領域番号が1であれば、図11のテーブルの領域番号1のエントリを参照し、空き領域の有無を確認する。図11に示す例では、「有」であり、空きがあることを示している。

【0085】空き領域のある使用可能なリソース領域が見つかった場合（ステップS43でYes）にはそれを結果として返す（ステップS45）。リソース領域が見つからない場合（ステップS43でNo）は、リソース領域がないことを結果（例えば0を使用する）で返す（ステップS46）。

【0086】（コネクション管理）上述した3つのフェーズによるコネクション決定により、利用者に応じたリソースが割り当てられてコネクションが確立することになる。本発明の通信処理装置は、リソース領域毎のコネクションの管理をリソース領域対応テーブル（図5、101）を用いて実行する。なお、図5においてリソース領域対応テーブル101は、TCPコネクション処理用リソース150内に示され、リソースとして適用されるメモリ内にテーブルを格納する構成として示されているが、リソース領域対応テーブル101は、外部の記憶装置140に格納する構成としてもよい。

【0087】図13にリソース領域対応テーブルのデータ構成例を示す。リソース領域対応テーブルは図13に示すように、送信元のIPアドレスまたはポート番号、または両者の組合わせデータからなるエンドポイントと、コネクションに使用されているリソース領域番号とを対応付けたテーブルとして構成される。

【0088】このテーブルにおいて、通信端末装置が実行中のコネクション数、使用リソース領域番号が取得され、例えばリソース領域対応テーブルのあるリソース領域に対応して設定されたコネクション数が前述のリソース管理情報テーブル（図11参照）の最大コネクション数に等しくなった場合は、リソース管理情報テーブルの「空き領域の有無」のデータフィールドが「有」から「無」に更新されることになる。

【0089】以上、説明したように、リソース決定処理例1は、

第1フェーズ：TCPコネクション要求のトラフィックデータの情報から利用者を識別、または利用者及び利用するサービスの双方を識別する利用者識別処理、

第2フェーズ：識別された利用者に応じて、リソースの使用条件を与えるリソース使用条件決定処理、

第3フェーズ：リソース使用条件から使用するリソース領域を決定するリソース領域決定処理、

これらの3フェーズからなるリソース決定処理により、利用者に応じてリソース領域の使用を制限することを可能としている。従って、優先度の低いユーザは一部のリソース領域しか使用できないが、優先度の高いユーザは全リソースを使用できるといった条件付けが実現できる。

【0090】なお、上述の説明では、利用者としてコネクション要求元、すなわち送信元IPアドレス、送信元MACアドレスに基づいて利用者識別を行なう処理例について説明したが、さらに、SYNパケットのヘッダ情報から送信先ポート番号を取得して、送信先ポート番号に応じたリソースの割り当てを実行する構成としてもよい。本構成とすることにより、送信先ポート番号、すなわちプロトコルに応じてリソースの使用率を設定することが可能となる。

【0091】[リソース決定処理例2]次に、利用者ごとにコネクション数を制限して、優先度に応じた利用者毎のコネクションの設定可否を判定する構成について、リソース決定処理例2として説明する。

【0092】図14に、通信処理装置に対するTCPコネクション要求に対して、通信処理装置において通信処理制御を実行する制御手段の実行するリソース決定処理の詳細を説明する図を示す。

【0093】TCPコネクション処理用リソース250は、TCPトラフィック処理用のリソース（メモリ領域、ディスク領域）をまとめて示している。リソース250は、先に説明したリソース決定処理例1とは異なる

り、複数の領域に分割されたものとはなっていない。

【0094】図14に示すリソース使用可能判定処理部230は、2つの処理フェーズa、bを実行する。処理フェーズaは、前述のリソース決定処理例1における第1フェーズと同様、TCPコネクション要求のトラフィックデータの情報から利用者を識別、または利用者及び利用するサービスの双方を識別する利用者識別処理である。処理フェーズbは、リソース決定処理例2に固有の処理であり、ユーザID毎に対応付けられた設定可能なコネクション数と現コネクション数を比較し、ユーザID毎に対応付けられた設定可能なコネクション数を超えない場合は、コネクションを確立させ、超える場合は、他のユーザIDに対応して設定されたコネクション数に空きがあるかを判定し、空きがある場合にコネクションを確立させる処理を実行する。

【0095】図14に示すように、2つのフェーズの処理、すなわち、利用者識別処理、リソース使用条件決定処理において、記憶装置240に記憶された各テーブル、すなわち利用者テーブル211、リソース使用条件テーブル212を参照した処理が実行される。これらの各テーブルに対する情報格納、更新処理は、それぞれ利用者設定処理部221、リソース使用条件設定処理部222が行なう。また、リソースの使用状況を管理するためにリソース使用状況テーブル201が使用される。

【0096】以下、各テーブル構成例を図面に示し、図を参照しながらリソース使用可能判定処理部230におけるリソース使用可能判定処理の各フェーズにおける処理の詳細について説明する。

【0097】（フェーズa：利用者識別処理）利用者識別処理は、通信処理装置が受信したSYNパケットから利用者、すなわち通信処理装置に対して接続要求を行ってきた通信要求者、あるいは通信要求端末を識別する処理である。この利用者識別処理は、前述のリソース決定処理例1における第1フェーズと同様の処理であるので詳細な説明は省略する。

【0098】すなわち、TCPコネクション要求のトラフィックデータの情報から利用者を識別、または利用者及び利用するサービスの双方を識別する利用者識別処理であり、利用者テーブル（図7参照）を参照した処理として実行され、利用者テーブルから利用者IDを取得する処理として実行される。

【0099】（フェーズb：リソース使用条件決定処理）リソース使用条件決定処理は、上述の利用者識別処理において識別された利用者に応じて、リソース使用条件を決定する処理である。このリソース使用条件決定処理は、リソース使用条件決定テーブル212を参照した処理として実行される。

【0100】リソース使用条件決定テーブルの構成例を図15に示し、リソース使用条件決定テーブルを参照したリソース使用条件決定処理の処理フローを図16に示

す。リソース使用条件決定テーブルは、図15に示すように、グループID、利用者IDに対して、リソース使用条件としての使用可能な最大コネクション数、および現在のコネクション数を対応付けたテーブルとして構成される。

【0101】グループIDはリソース使用条件を識別するための識別子（ID）である。利用者IDはこのグループIDに所属する利用者IDのリストである。同じ利用者IDが複数のグループIDに含まれることが可能である。最大コネクション数は各グループID内の利用者に接続を許す最大のコネクション数である。現在のコネクション数は、そのグループIDに属する利用者によって使用され接続している現在のコネクション数を表す。

【0102】あるコネクション要求に対して、コネクション確立の可否を判定する場合は、フェーズaにおいて取得した利用者IDに基づくリソース使用条件決定テーブルの検索が実行される。テーブルの下グループIDから順に、フェーズaにおいて取得した利用者IDが含まれているかを確認し、利用者IDが含まれているグループIDで最大コネクション数より現在のコネクション数が小さければコネクション確立が可能でありそのグループIDのコネクションとして接続する。

【0103】図16を参照して、リソース使用条件決定処理の処理について説明する。リソース使用条件決定処理は、前述のフェーズaの利用者識別処理の結果を取得して実行される。利用者識別処理の結果として、利用者IDを受け取り、その値に基づいて、リソース使用条件テーブル（図15）を一番下のグループIDのエントリから検索し、利用者識別処理で識別された利用者IDが各エントリに含まれるか否かを確認する（ステップS51）。

【0104】利用者識別処理の結果として取得した利用者IDが含まれたエントリが検索されると（S52でYes）、リソース使用条件決定テーブルの当該エントリの現在のコネクション数と最大コネクション数との比較処理を実行する（ステップS53）。

【0105】[現在のコネクション数]<[最大コネクション数]の場合（ステップS54でNo）は、使用可能なリソースが存在すると判断し、リソース使用条件決定テーブルの当該エントリに対応付けられたグループIDを返す（ステップS55）。

【0106】利用者識別処理の結果として取得した利用者IDが含まれていないエントリである場合（S52でNo）、もしくは利用者識別処理の結果として取得した利用者IDが含まれているエントリにおいて、現在のコネクション数=最大コネクション数の場合（ステップS54でYes）には、リソース使用条件決定テーブルの一つ上のグループIDのエントリを調べる（ステップS56）。このループを繰り返し、リソース使用条件決定テーブルの全てのグループIDに対応するデータエント

リを調べても利用者識別処理の結果として取得した利用者 ID が含まれたエントリが見つからなかった場合、あるいは利用者 ID が含まれたエントリであっても現在のコネクション数=最大コネクション数のエントリしか存在しなかった場合には使用可能なリソースが見つからなかったことを示す null を返す (ステップ S 58)。

【0107】リソース使用条件決定処理の後、結果が null であれば、使用可能なリソースがないため、この TCP コネクション要求の SYN パケットは棄却される。リソース使用条件決定処理結果としてグループ ID が取得されれば、通常どおりの TCP コネクション要求処理が行われる。

【0108】(コネクション管理) 上述した 2 つのフェーズによるコネクション決定により、利用者に応じたリソースが割り当てられてコネクションが確立することになる。本実施例の通信処理装置は、リソース領域毎のコネクションの管理をリソース使用状況テーブル (図 14、201) を用いて実行する。

【0109】図 17 にリソース使用状況テーブルのデータ構成例を示す。リソース使用状況テーブルは図 17 に示すように、送信元の IP アドレスまたはポート番号、または両者の組合わせデータからなるエンドポイントと、コネクションに使用されているグループ ID とを対応付けたテーブルとして構成される。

【0110】TCP コネクション処理用のリソース確保時に、TCP コネクション処理はリソース使用状況テーブルに、コネクションのエンドポイントとリソース使用条件決定処理の結果のグループ ID を書き込み、リソース使用条件テーブルにおけるそのグループ ID に対応する現在のコネクション数を 1 増加させる。

【0111】また、コネクションの終了時には、リソースを開放する際に、図 17 に示すようなリソース使用状況テーブルを閲覧してこのコネクションのエンドポイントに対応するグループ ID を得て、リソース使用条件テーブルのそのグループ ID に対応する現在のコネクション数を 1 減少させる。その後、リソース使用状況テーブル中のこのコネクションに関するエントリを消去する。

【0112】以上、説明したように、リソース決定処理例 2 は、

フェーズ a : TCP コネクション要求のトラフィックデータの情報から利用者を識別、または利用者及び利用するサービスの双方を識別する利用者識別処理、

フェーズ b : ユーザ ID 毎に対応付けられた設定可能なコネクション数と現コネクション数を比較し、ユーザ ID 毎に対応付けられた設定可能なコネクション数を超えない場合は、コネクションを確立させ、超える場合は、他のユーザ ID に対応して設定されたコネクション数に空きがあるかを判定し、空きがある場合にコネクションを確立させる処理、これらの 2 フェーズからなるリソース決定処理により、利用者に応じて確立コネクション数

を制限することを可能としている。従って、優先度の低いユーザは少ないコネクション数しか使用できないが、優先度の高いユーザは多くのコネクションを使用できるといった条件付けが実現できる。このように、利用者ごとにコネクション数を制限することができ、利用者を複数のグループ ID に所属させることにより、柔軟なコネクション数制限が可能となる。

【0113】なお、上述の説明では、利用者としてコネクション要求元、すなわち送信元 IP アドレス、送信元 MAC アドレスに基づいて利用者識別を行なう処理例について説明したが、さらに、SYN パケットのヘッダ情報から送信先ポート番号を取得して、送信先ポート番号に応じたリソースの割り当てを実行する構成としてもよい。本構成とすることにより、送信先ポート番号、すなわちプロトコルに応じて確立コネクション数を設定することが可能となる。

【0114】[通信処理装置構成例] 次に通信処理装置の構成例について図 18 を用いて説明する。図 18 には、通信処理装置の構成例を示す。CPU (Central processing Unit) 501 は、各種アプリケーションプログラムや、OS (Operating System) を実行する演算ユニットである。ROM (Read-Only-Memory) 502 は、CPU 501 が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。RAM (Random Access Memory) 503 は、CPU 501 の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【0115】ホストバス 504 はブリッジ 505 を介して PCI (Peripheral Component Internet/Interface) バスなどの外部バス 506 に接続されている。

【0116】キーボード 508 は CPU 501 に各種の指令を入力するためにユーザにより操作され、ポインティングデバイス 509 はディスプレイ 510 の画面上の位置指定、コマンド指定などの際にユーザによって操作される。ディスプレイ 510 は例えば CRT、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。HDD (Hard Disk Drive) 511 は、情報記憶媒体としてのハードディスクを駆動し、ハードディスクからのプログラム、データの読み取りまたはハードディスクに対するプログラム、データの書き込みを実行する。

【0117】ドライブ 512 は、フロッピー (登録商標) ディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magneto optical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体 513 の記録再生を実行するドライブであり、各リムーバブル記録媒体 513 からのプログラムまたはデータ再生、リムーバブル記録媒体 513 に対するプログラムまたはデータ格納を実行する。

【0118】各記憶媒体に記録されたプログラムまたはデータを読み出してCPU501において実行または処理を行なう場合は、読み出したプログラム、データはインタフェース507、外部バス506、ブリッジ505、ホストバス504を介して例えば接続されているRAM503に供給する。

【0119】キーボード508乃至ドライブ512はインタフェース507に接続されており、インタフェース507は外部バス506、ブリッジ505、およびホストバス504を介してCPU501に接続されている。

【0120】通信部514は通信処理装置の接続された例えばルータ等を介して他の端末またはサーバと通信し、CPU501、HDD511等から供給されたデータをパケット化して送信したり、ルータを介してパケットを受信する処理を実行する。通信部503は外部バス506、ブリッジ505、およびホストバス504を介してCPU501に接続されている。

【0121】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0122】なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【0123】例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magneto optical)ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0124】なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の

記録媒体にインストールすることができる。

【0125】なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0126】

【発明の効果】以上、説明したように、本発明の通信処理装置、および通信処理方法によれば、コネクション要求の利用者を識別し、識別された利用者に応じて設定されたリソースの使用条件に従って使用するリソース領域を決定する構成としたので、優先度の高い利用者を使用可能なリソースを多く設定するなどの処理により、不特定多数の利用者からのコネクション要求がある通信処理装置において、特定のユーザに対して優先的にコネクションを確立することが可能となる。

【0127】また、本発明の通信処理装置、および通信処理方法によれば、利用者に応じて利用可能なコネクション数を設定し、識別された利用者に応じて設定されたコネクション設定数に従ってコネクションの可否を判定する構成としたので、優先度の高い利用者を使用可能なコネクションを多く設定する処理により、不特定多数の利用者からのコネクション要求がある通信処理装置において、特定のユーザに対して優先的にコネクションを確立することが可能となる。

【0128】また、本発明の通信処理装置、および通信処理方法において、利用者情報としてコネクション要求元のIPアドレス、MACアドレス、さらに送信先ポート番号を取得して、送信先ポート番号に応じたリソースの割り当てを実行する構成によれば、送信先ポート番号、すなわちプロトコルに応じたリソースの使用率を設定し、利用に応じた優先使用の設定をすることが可能となる。

【0129】また、本発明の通信処理装置、および通信処理方法によれば、複数の優先度の低い利用者により、多量のTCPコネクションが確立されたり、優先度の低い利用者から、TCPトラフィック処理用のリソースに対するDOS攻撃が行われて、コネクションの確立が困難になるなどの状況の発生を効果的に防止することが可能となる。

【図面の簡単な説明】

【図1】TCPコネクションの処理の概要を説明する図である。

【図2】IPパケットにおけるTCPヘッダの構成を説明する図である。

【図3】IPパケットにおけるIPヘッダの構成を説明する図である。

【図4】本発明の通信処理装置におけるTCPコネクション要求処理の処理概要を説明するフロー図である。

【図 5】本発明の通信処理装置における TCP 接続要求処理の処理概要を説明する図である。

【図 6】本発明の通信処理装置におけるリソース領域選択処理の処理概要を説明するフロー図である。

【図 7】本発明の通信処理装置における利用者識別処理において適用される利用者テーブルの構成例を示す図である。

【図 8】本発明の通信処理装置における利用者識別処理を説明するフロー図である。

【図 9】本発明の通信処理装置におけるリソース使用条件決定処理において適用されるリソース使用条件テーブルの構成例を示す図である。

【図 10】本発明の通信処理装置におけるリソース使用条件決定処理を説明するフロー図である。

【図 11】本発明の通信処理装置におけるリソース領域決定処理において適用されるリソース管理情報テーブルの構成例を示す図である。

【図 12】本発明の通信処理装置におけるリソース領域決定処理を説明するフロー図である。

【図 13】本発明の通信処理装置における接続管理処理において適用されるリソース領域対応テーブルの構成例を示す図である。

【図 14】本発明の通信処理装置における TCP 接続要求処理の処理概要（例 2）を説明する図である。

【図 15】本発明の通信処理装置におけるリソース使用条件決定処理（例 2）を説明するフロー図である。

【図 16】本発明の通信処理装置におけるリソース領域決定処理（例 2）において適用されるリソース管理情報テーブルの構成例を示す図である。

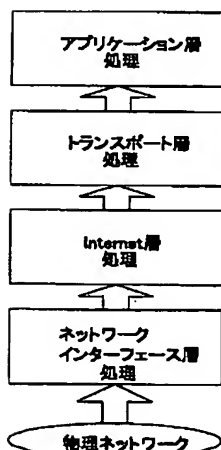
【図 17】本発明の通信処理装置における接続管理処理（例 2）において適用されるリソース使用状況テーブルの構成例を示す図である。

【図 18】本発明の通信処理装置の構成例を示す図である。

【符号の説明】

- 101 リソース領域対応テーブル
- 111 利用者テーブル
- 112 リソース使用条件テーブル
- 113 リソース管理情報テーブル
- 121 利用者設定処理部
- 122 リソース使用条件決定処理部
- 123 リソース設定処理部
- 130 リソース決定処理部
- 140 記憶装置
- 150 TCP 接続処理用リソース
- 201 リソース使用状況テーブル
- 211 利用者テーブル
- 212 リソース使用条件テーブル
- 221 利用者設定処理部
- 222 リソース使用条件決定処理部
- 230 リソース使用可能判定処理部
- 240 記憶装置
- 250 TCP 接続処理用リソース
- 501 CPU (Central processing Unit)
- 502 ROM (Read-Only-Memory)
- 503 RAM (Random Access Memory)
- 505 ブリッジ
- 508 キーボード
- 509 ポインティングデバイス
- 510 ディスプレイ
- 511 HDD
- 512 ドライブ
- 513 リムーバブル記憶媒体
- 514 通信部

【図 1】

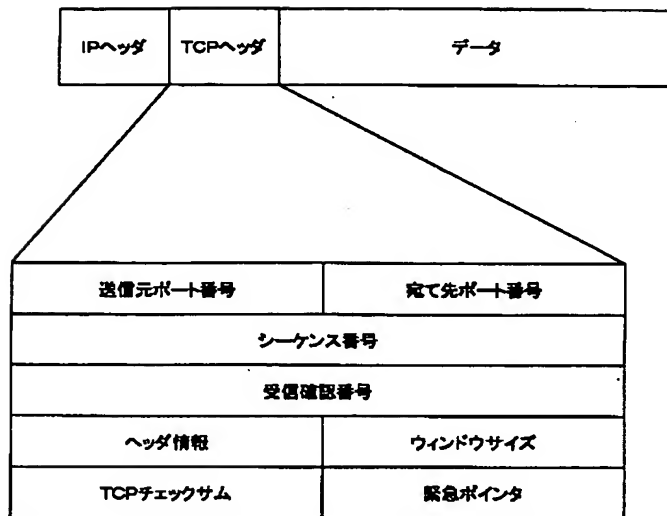


【図 7】

利用者テーブル

利用者ID	送信元MACアドレス	送信元IPアドレス	送信先ポート番号
所有者ユーザ	35.42.1.56.1375		
友人A		45.67.123.245	
一般		42.134.78.95	80

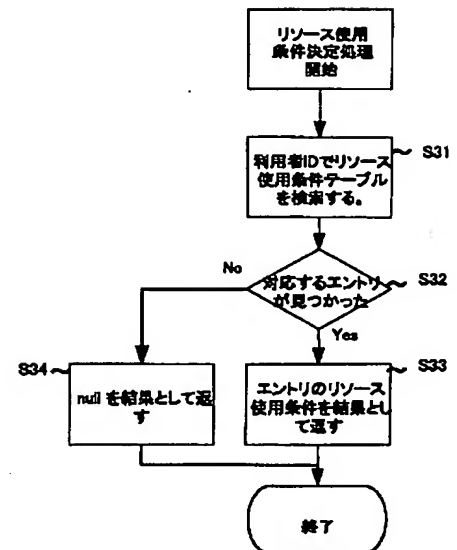
【図2】



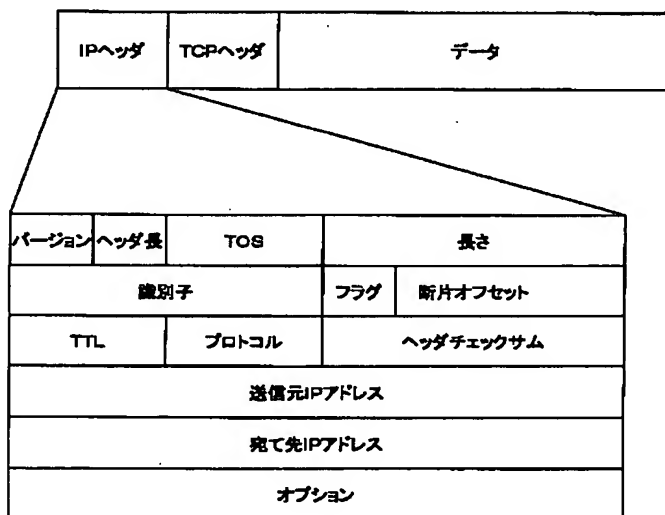
【図9】

利用者ID	リソース使用条件
所有ユーザ	1-9
友人A	3-9
一般	8-9
null	9

【図10】



【図3】

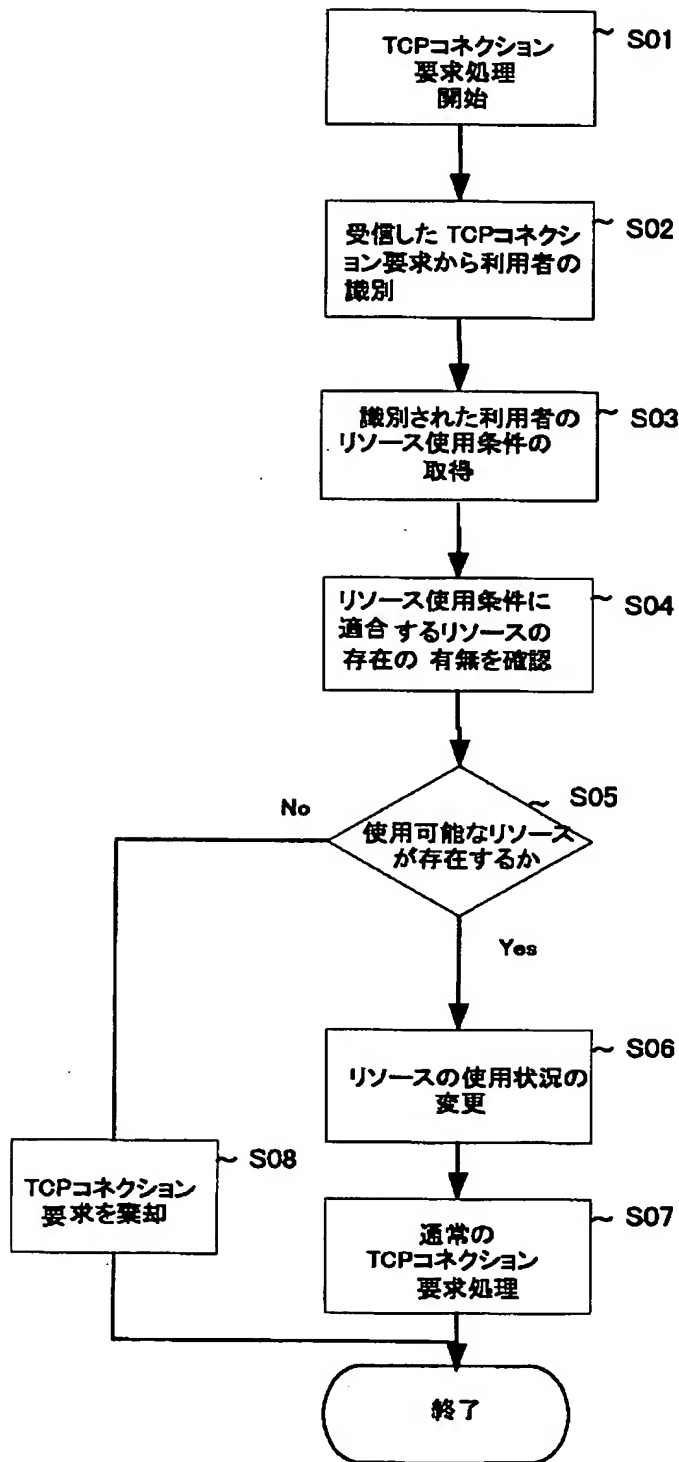


【図11】

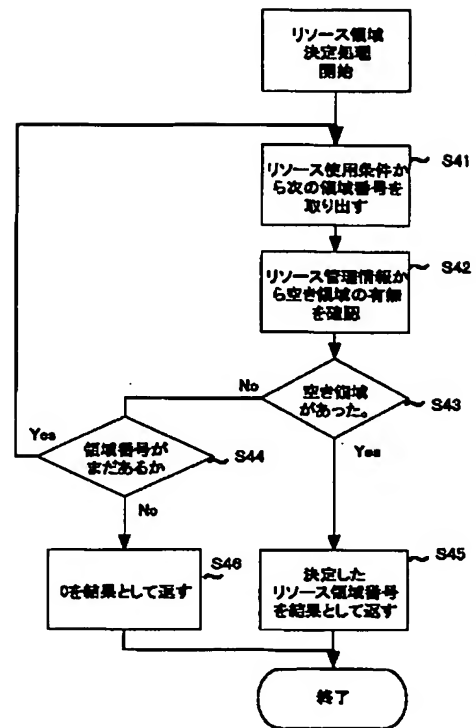
リソース管理情報テーブル

リソース領域番号	最大コネクション数	受信キューサイズ	空き領域の有無	リソース領域開始アドレス
1	20	5	有	0xFFFF8000
2	40	10	無	0xDFFF8000
...				
9	100	20	有	0xCFFF4000

【図 4】



【図 12】

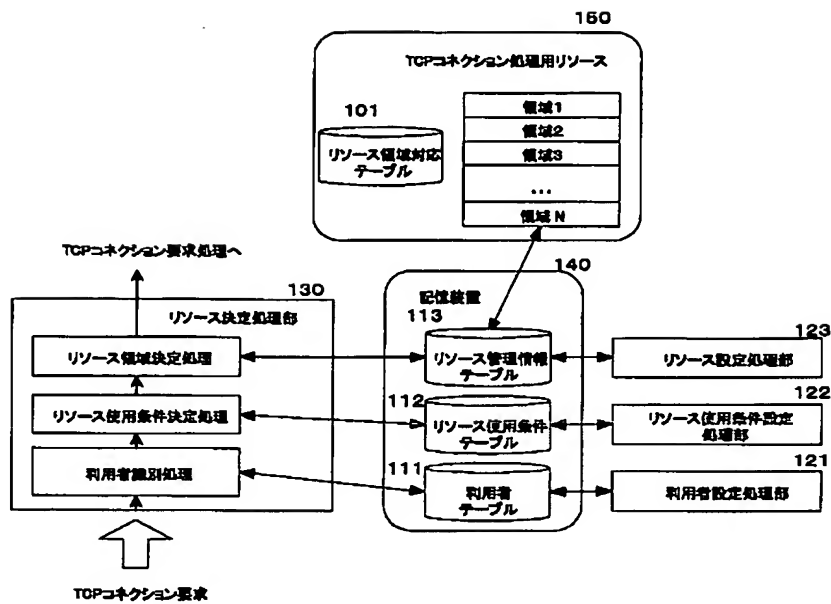


【図 13】

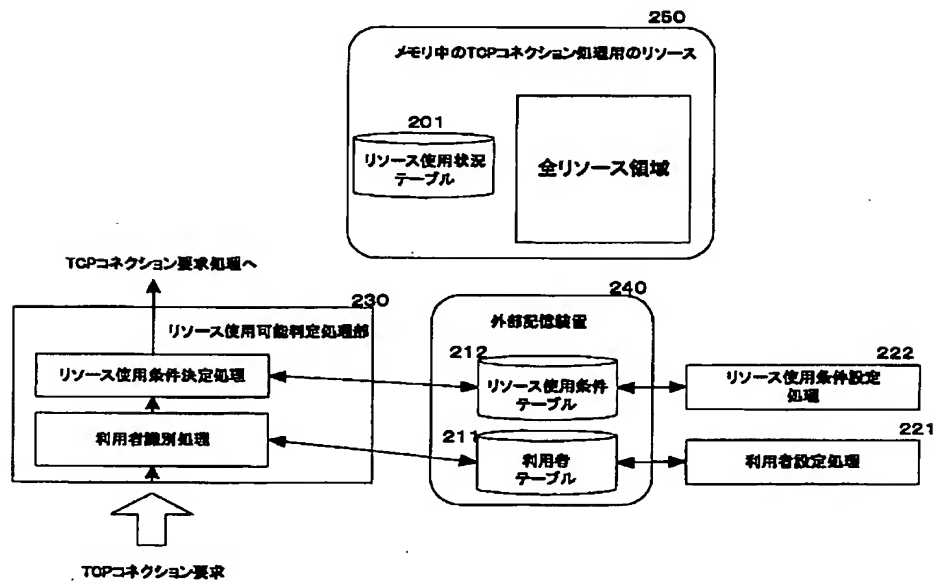
リソース領域対応テーブル

エンドポイント	リソース領域番号
(42.14.53.235,80)	1
(32.14.53.232,80)	9
...	...

【図5】



【図14】

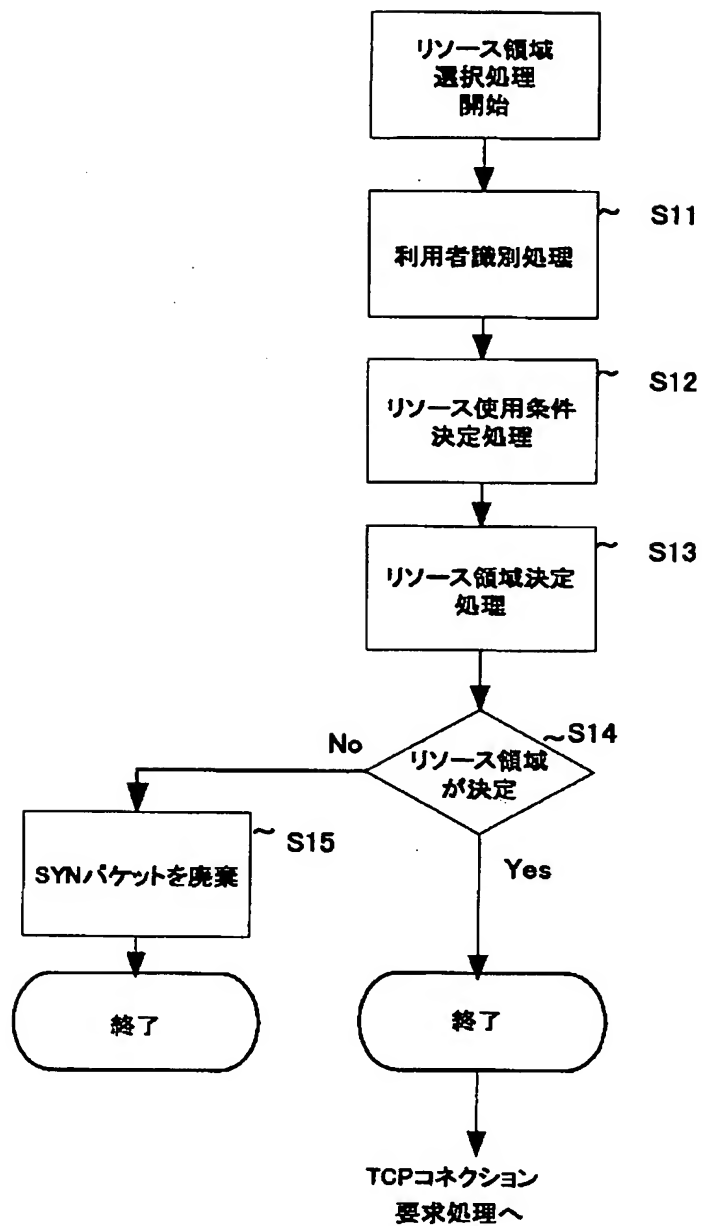


【図17】

リソース使用状況テーブル

エンドポイント	グループID
(42.14.53.235,80)	所有者Gp
...	...

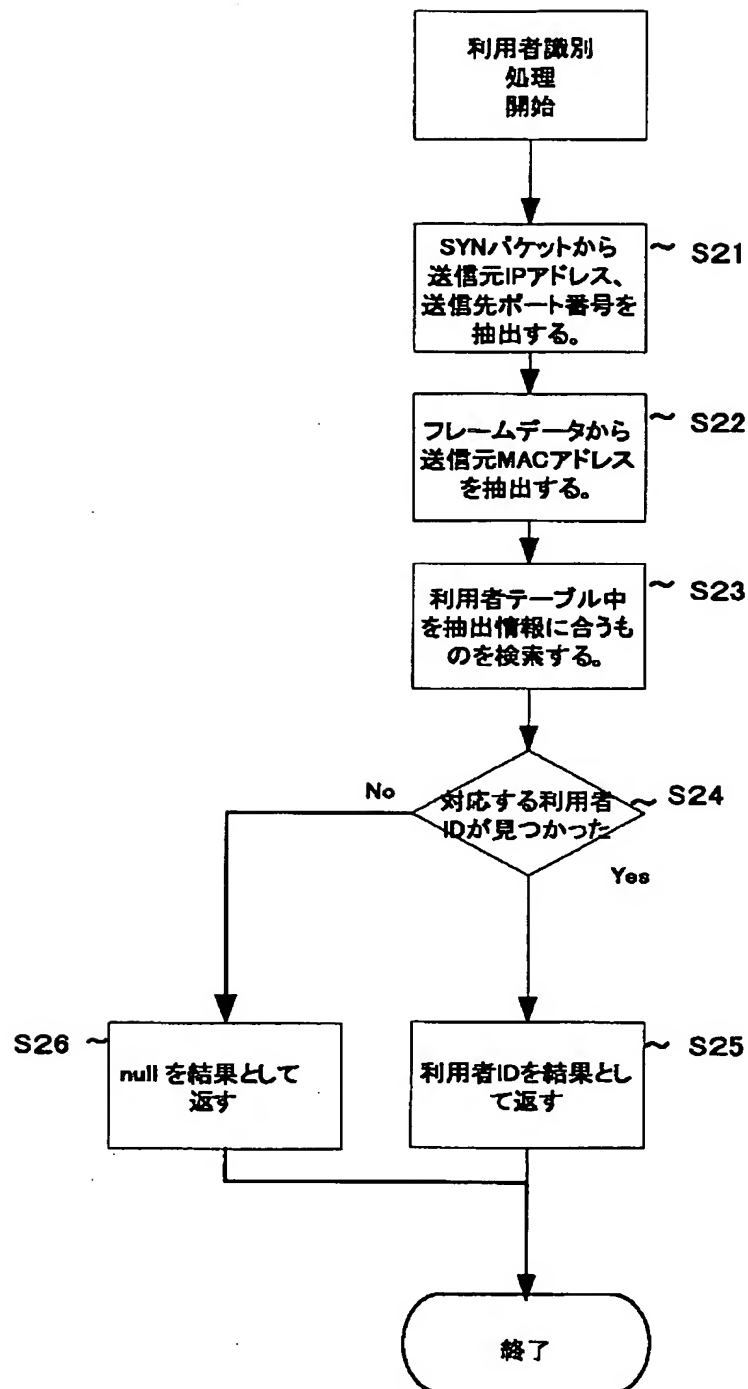
【図 6】



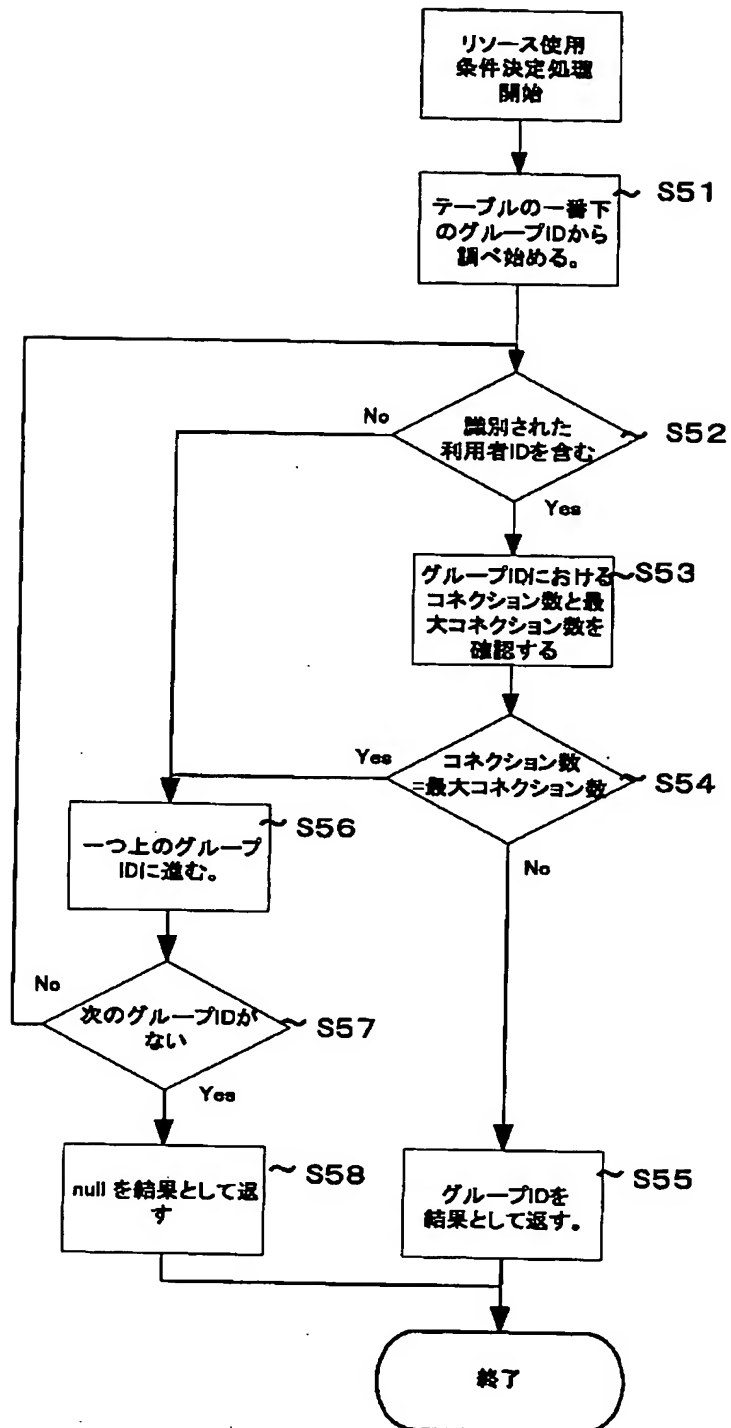
【図 15】

グループID	利用者ID	最大コネクション数	現在のコネクション数
所有GP	所有者	20	10
友人GP	所有者	10	10
	友人A		
一般GP	一般	5	4

【図8】



【図16】



【図18】

